Is the Software capable of accurately detecting and recording copies of data being shared from a Subscriber's IP Address taking place on BitTorrent networks?

11.2 Based on my examination of the source code presented and the tests performed, the System correctly detects and records instances of copies of data being shared from a Subscriber's IP address on the BitTorrent networks.

11.3 It accurately records the IP addresses, port numbers, time stamps and the SHA-512 hash value of the sub-pieces received by the System in a secure database.

How does the System function?

11.4 The Software consists of various modules. Each of the modules has a distinctive task including (but not limited to) tracking IP traffic, calculating hash values and recording the correct time.

11.5 When the System is initiated, it checks the operating system, interfaces, clock and memory on the computer on which the Software is installed for potential errors. If any potential errors are identified, the Software and thus the System does not function.

11.6 The System ensures that an accurate time is used by calibrating its local clock with various NTP servers. The System uses amongst others, the time signals distributed by the Physikalisch-Technische Bundesanstalt (the German national metrology institute).

11.7 The System captures all data packets being transmitted between the local BitTorrent Client and a remote one. Once the local BitTorrent Client receives information about the availability and location of distributed data, it will initiate communications with those locations.

11.8 A TCP connection is then initiated by the local BitTorrent Client in order to inform source computers that the System is interested in acquiring data. Once transfer begins, all data traffic is accurately recorded with information such as time of the data transfer, IP addresses, port numbers, and if the parties in the TCP connection wish to send or receive data. If a data transfer between the System and remote computer is successful, the IP address is logged, together with time stamp and the port number used by the source computer.

11.9 Information is logged by the System only if the TCP connection is active two seconds before and after the data transfer. This ensures that users participating in transactions for a lesser period of time are not logged. This adequately addresses the issue of a dynamic IP address changing.

11.10 The hash value of the transmitted sub-piece is also recorded by the System.

11.11 Once the connection between the System's local BitTorrent Client and the source computer is closed the data captured is transferred to a secure database. The storage medium is a write-once read only. The database is backed up once per day. The backup carries a time stamp and is secured by a digital signature.

Is there a likelihood for erroneous information to be recorded by the System?

11.12 It is impossible for the System to record erroneous information. The System uses the TCP protocol to establish a communication channel with source computers. By design, the connections established are valid. If a TCP connection is not initiated between the System and source computer then no data is logged.

11.13 The System also checks the hash values of all sub-pieces received to ensure they are part of the full file.

11.14 If any technical problems or errors, including those described at paragraph 7.3 above, occur during the data capture and logging process, the relevant process is terminated and data captured during that process is not transferred to the secure database. This means that all data transferred to the secure database and stored by the System is error free.

Can the information recorded by the System be manipulated by a user?

11.15 This may be possible in limited circumstances where an individual has access to the database and the backup files with the required security clearance and the possession of the key to the digital signature.

11.16 The risk of database manipulation is mitigated as the database records all access to it. Those records may be used to trace unauthorised access to the user account responsible. As an added security measure, the backup files are secured by digital signatures.

11.17 The System saves all network traffic between the system and the remote computer. Manipulation of this without detection is difficult to accomplish given the security measures in place.

11.18 I consider the above stated limited circumstances are impossible to achieve.

When the System engages in a BitTorrent transaction with a remote computer, is the System able to accurately record the IP address of the remote computer and date and time?

11.19 The System is able to accurately record the IP address and the associated time stamp.

11.20 When a remote computer offers to distribute a piece of data to the System, both parties must establish a secure end-to-end connection using the TCP/IP protocol. When a transfer takes place, the IP address of the remote computer is logged by the System.

11.21 NTP servers ensure that the System receives accurate time information. This allows the System to accurately calibrate its clock. The System uses its clock to produce data transfer time stamps.

11.22 Using an IP address and associated time stamp of the data transfer, an ISP may correctly identify the Subscriber allocated that IP address at a specific time by searching databases in its possession. Most ISPs will operate a data retention policy. This means that the information

sought may be deleted after a period of time. It is therefore important for copyright owners who allege that the data transfer captured by the System contains copyrighted material to obtain disclosure of the names and addresses behind the IP addresses before such deletion occurs.

What is the link between hash value and IP address, and does the System record this information accurately?

11.23 When a remote computer responds to the local client's request for data, the remote computer will begin to transfer a sub-piece of the requested file. This data transfer is monitored and recorded by the System. Once the complete sub-piece is received successfully by the System, a record in the database is created documenting that transaction.

11.24 The database record contains all information relating to the transaction between the System and source. That information includes the following:

(a) IP address of the sender;

(b) IP address of the System;

(c) port numbers used for the transfer;

(d) time stamps for:

(i) the start of the conversation;

(ii) the end of the conversation;

(iii) the start and end of the download;

(e) the SHA-512 hash value of the data received from the source computer; and

(f) the position of the sub-piece in the complete file.

11.25 Once the above information has been logged, a hash value comparison is initiated by the System. The hash value of the sub-piece received from the source computer is calculated and compared to the hash value of the complete data set of the copyrighted work stored in a reference file. If the hash values and positions are the same, the System establishes that the downloaded sub-piece must have been part of the copyrighted work. In my opinion, this is the correct finding to make in the circumstances.

What procedures are in place to ensure that the IP address recorded was allocated to the correct Subscriber at the time of the alleged copyright infringement?

11.26 The Subscriber may be identified with the assistance of the ISP responsible for the allocation of that IP address. Only the ISP stores this information. Without the ISP's assistance, a copyright owner cannot identify the Subscriber.

11.27 In the case of dynamic IP addresses, various Subscribers may have the same IP address – but during different time periods. This is the reason it is important that the correct time stamp is recorded accurately by the System once an infringement of copyright is detected.

11.28 To ensure a correct time stamp the System synchronizes its time with NTP servers, which allows the System to produce accurate time stamps.

11.29 Logs with more than a 10 milliseconds time difference are not exported by the Software for use as evidence in legal proceedings, as these have the possibility of introducing potential inaccurate logs into the database. This scenario is avoided altogether by rejecting such logs. In my opinion, these safety protocols ensure that the Software produces accurate time stamps.

11.30 As the System establishes a connection to the source for at least 2 seconds after the successful data transfer, the accuracy of the time stamp recorded for the data transfer is valid.

What is the 'anti-leech mod' and how does it affect the System's reliability?

11.31 Within a P2P Network, users exchange data amongst themselves. A BitTorrent Network is a type of P2P network. It relies on the willingness of all participants to share their data. If a client is not sending data it will be marked as a 'leecher'. The System does not log users known as "leechers". A leecher is a user who does not act as a data source. The System only enters into transactions with those users who engage in the distribution of data. In other words, the users logged by the System have not only made available data, but also engaged in an actual transaction with the System and has been recorded distributing a piece of the data.

11.32 In the operation of the System, the local BitTorrent Client is created in a way which ensures that it never transfers pieces of copyrighted files to other users. Instead, the client in the System mimics a user willing to act as a source of data but no actual transfer takes place. It does not affect the accuracy or reliability of data logging by the System.

What are dynamic IP addresses and what effect (if any) do these have on the accuracy of the information recorded by the System?

11.33 An explanation of dynamic IP addresses may be found in section 6. In summary, an ISP may assign an IP address to different Subscribers at different periods of time. But as the time of the data transfer is recorded accurately by the System, an ISP is able to determine which Subscriber it assigned an IP address to at a particular moment in time using the IP address and time stamp.

What are hash collisions and how do they affect the accuracy of the information recorded by the System?

11.34 A hash collision occurs when two different data sets have the same hash value. The System uses the SHA-512 method to determine the hash value of the sub-piece transferred.

11.35 There are two potential sources of hash collisions:

(a) Trivial hash values, being:

(i) hash values calculated from a file containing either bit values of 0 or 1 or the same data in each block; and

(ii) bit patterns that describe the type of the file transferred.

The System checks the hash values against a blacklist and other trivial data sets. Data transfers involving these hash values are deleted by the System and are not logged.

(b) Hash collisions for the complete file and a sub-piece

The System identifies files by their name and SHA-1 hash value. It checks the value of the SHA-512 hash value of the downloaded sub-pieces against the calculated SHA-512 hash value of the reference file. To perform this calculation the position of the sub-piece must also be known. The probability of the same data of two different files being at the same place is extremely unlikely. This means that where the hash value and location match, it may be said that distribution of the relevant data set took place.

11.36 Thus, in my opinion, the System addresses the risk of trivial hash collisions and treats them correctly by not recording the transaction.

Does the System download from a source computer the full file?

11.37 The connection with a source is terminated after the System receives a sub-piece of the copyrighted work from the source. The System may connect with the same source again in relation to another sub-piece of the same work. However, the System does not acquire the whole file from a single source. This is not necessary or always possible.

11.38 However, each user does make the Complete Data Set available for download to other users. While it is possible for a user to make only one piece of the Complete Data Set available, this is extremely unlikely, as the user would need to possess highly specialised information technology skills to split a Complete Data Set into several pieces and make each piece available for download separately. This is also highly unlikely because users on the BitTorrent network are using BitTorrent network to download and make available Complete Data Sets, such as complete movies.

11.39 Users of BitTorrent networks seek to acquire various files. These may include copyrighted works such as movies, software and music. In relation to movies, the intention of a user is to acquire a full copy of a movie. It would be nonsensical to acquire only one piece, which may only be a few random seconds of the movie. When a user acquires software, it is unlikely that the software will function properly or even install if it is incomplete. A user therefore needs to acquire the Complete Data Set for the software in order to use it. Furthermore, in relation to music files, it is inconceivable that a user will only seek to acquire a random few seconds of a musical work.

11.40 BitTorrent users have little control over which pieces they acquire first. They acquire the pieces that are available and offered by other users. For these reasons, it is reasonable to say that

those wishing to acquire a file will participate in a BitTorrent network until the Complete Data Set is acquired.

11.41 A user who has acquired the Complete Data Set will continue to transmit pieces of that file to other users unless the client is instructed to stop doing so. It is not uncommon for users to continue distributing the files for long periods of time.

11.42 A user without the full data set will request the pieces it does not have from other sources. These transmissions may take place while that user is transmitting data to the System. Accordingly, the possession and distribution of a sub-piece is a very strong indication that the user is or will in the future be in the possession of the complete data set.

11.43 The reason why P2P Networks work so quickly and effectively is because different parts of a movie are obtained from different users until an entire film is downloaded. That is, when downloading a movie the user's computer may simultaneously download the movie from a number of different other peers' computers.

12. Declaration

I, Dr Simone Richter, declare that I have made all the inquiries that I believe are desirable and appropriate and that no matters of significance that I regard as relevant have, to my knowledge, been withheld from the Court.

Signature..... Date... 2 April 2014

Dipl.-Phys. Dr. Simone Georgia Richter
Sachverständige für Systeme und Anwendungen der Informationsverarbeitung
Von der Industrie- und Handelskammer öffentlich bestellte und vereidigte Sachverständige

Dr. Simone Richter
permanently sworn in and officially installed expert witness for Systems and Application of Information Technologies. Officially supervised by the Chamber of Commerce in Darmstadt

Appendix A

Curriculum Vitae

Name: Dr. rer. nat. Simone Richter

Born: December 13, 1969 in Berlin, Germany

Career Summary

Over the past 15 years of professional experience, I have gained extensive knowledge and expertise in the following areas:

- General and extended IT-knowledge
- Company Administration (Finance, Controlling, Human Resources, Technology Transfer, Legal, Site & Buildings, Risk Management, Quality Management, Procurement and Contracts)
- General Project Management
- Strategy Development and Deployment
- Change Management
- Technical Project Management
- Project Team Management
- ERP Project Management
- Project Evaluation
- Particle Accelerator Design and Operations

Due to my training and experience, I have specialised knowledge in all areas of I.T including computer hardware, software, data centres, networking and database management.

Since January 2003, I have provided independent expert witness testimony in Germany as an accredited I.T. expert. This accreditation is provided by the German government to individuals who demonstrate through rigorous testing, that they have the qualifications, training and experience to provide expert opinions and Court approved reports for the benefit of the Court in the field of IT.

Education / Training

2010 – 2011	Malik Master of Management, MZSG St. Gallen, Switzerland
2008 – 2010	Certificate, Helmholtz-Akademie für Führungskräfte – Helmholtz Management Academy, Germany

2002 – 2005	Certificate, Medical Physics and Technics, University of Kaiserslautern, Germany
2001	Dr. rer. nat. - PhD, Technical University Darmstadt, Germany. My phD
1996	Diploma –Master with Thesis in Physics, Technical University Darmstadt, Germany. My diploma involved writing approx. 8,000 lines of code
1988	Abitur – university-entrance diploma , Göttenbach-Gymnasium, Idar-Oberstein

Certifications and Accreditations

2009 –	Member of the Lenkungsausschuss Helmholtz-Akademie für Führungskräfte(Steering Committee of the Member of the Selection Committee for the Helmholtz-Gemeinschaft Deutscher Forschungszentren e.V. (Helmholtz Association - HGF) Mentoring Program
2009 – 2010	Elected Member of the GSI Wissenschaftlicher Ausschuss (internal scientific council)
2008 – 2010	Elected Deputy Chairwoman of the Wissenschaftlich-Technische Räte-Versammlung of Helmholtz-Gemeinschaft Deutscher Forschungszentren e.V. (HGF) (Committee of scientific-technical councils)
2006	Member of the Working Group "Strategy of the Helmholtz Gemeinschaft"
2005 – 2008	Chairwoman and Elected Member of the GSI Wissenschaftlicher Ausschuss
2004 – 2005	Member of the Internal Advisory Committee for the Definition of the Structure of the FAIR Project
2003 – 2004	Appointed Member of GSI Wissenschaftlicher Ausschuss
2003	Accreditation as expert witness (permanently sworn in as public officer) with formal knowledge examination according to German law §36 GewOo re-certified and renewed oath
2005, 2010	My involvement at the GSI's internal scientific council and later on also within the committee of scientific-technical councils at the HGF gave me the opportunity to work on the steering level of the organizations. The boards I led as chair or deputy chair are asked to give strategic advice to the managing and governing boards of the respective organizations. I gained a deep insight in decision making pro-

cesses with high profile stakeholders such as ministries or other representatives of large research organizations.

Work History

2003 – Present

In January 2003 I was formally sworn in as a public officer as an expert witness in all matters related to Information Technology. In this position, I am regularly called to provide technical expertise for Courts, public prosecuting offices and private organizations as an independent expert for the Court.

Prior to my accreditation, I was required to demonstrate my IT knowledge, by working on 10 different cases with another IT expert. After this, I was required to undertake a two day test which involved a written component in respect of General IT knowledge including hardware, software and operating systems, and then a practical component in which I was interviewed and my technical knowledge was tested by a 3 person panel. Upon passing these tests, I was recommended by the Darmstadt Chamber of Commerce to be accredited as an independent expert. Constant training is required to be reaccredited every 5 years. The chamber of commerce in Darmstadt, Germany serves as my supervising agency on behalf of the German government. Currently only approx. 140 individuals in Germany hold this accreditation.

Key Achievements

- Giving technical expertise reports and testimonies in civil court cases
- Providing IT-related expert opinions and court approved reports in private cases

General Responsibilities

- Working with judges, lawyers, plaintiff and defendant representatives to solve court cases
- Providing Companies with technical background information about IT-project statuses
- Evaluation of IT-project statuses
- Acting as public office for (IT) technical questions in and before court cases

2011 – Present **GSI Helmholtzzentrum für Schwerionenforschung GmbH; www.gsi.de**

Interims Manager

In-house Consultant and Strategic Advisor to the Administrative Managing Director

GSI GmbH as member of the German Helmholtz-Association (www.helmholtz.de) provides a heavy-ion particle accelerator as a national large-scale research infrastructure open to national and international scientists. The Helmholtz-Association is Germany's largest research organization with more

than 33.000 employees and ad yearly budget exceeding 3.4 billion €. GSI GmbH with a work force of approx. 1100 employees and a yearly budget of over150 M€/year is structured in two business units: the research and scientific and the administrative branch. I advise the Administrative Managing Director and interim manage the Organization and Controlling Division.

Key Achievements

- structuring and shaping of the Organization/Controlling Division and the Finance/Procurement Division initiating and guiding the change process for the Administration to a customer and project oriented division
- member of the task-force for Merger of GSI GmbH and FAIR GmbH
- member of the working group on the supervision of the FAIR GmbH
- interims management for the Organization/Controlling Division, coaching of the Head of the Finance and Purchasing Division, coaching of the department leader of the Patent and Technology transfer department, focusing on developing the IP-Policy
- requirements analysis for Controlling and Business Intelligence System.

General Responsibilities

- ensuring the process set-up for company-wide processes like budgeting, quality management, project management
- giving expertise on all FAIR related issues like in-kind contributions, project steering and control, reporting, and merging of FAIR with GSI
- giving expert advice to the CFO and the CEO of GSI

2010 – 2011 **Facility for Antiproton and Ion Research in Europe GmbH (FAIR GmbH), www.fair-center.org Administrative Managing Director, CFO.**

- The FAIR project represented by the FAIR GmbH is currently the largest European Research Project under construction. Its estimated cost to completion is 1.6 billion€, the envisaged start of operation is 2018.
- FAIR GmbH was founded under the umbrella of multinational treaty – The FAIR Convention. So far there are eight signatory countries to the Convention (Finland, France, Germany, India, Poland, Russia, Slovenia, and Sweden) and Spain expected to sign soon. The signatory countries are represented in the shareholders assembly through their respective nominated shareholders. For Germany the GSI GmbH is the major shareholder of FAIR. Shareholders contribute to the facility either in cash or in-kind. The FAIR accelerator facility complex will provide to more than 3000 scientists high precision heavy ion and antiproton beams at various experimental stations.

Key Achievements

- bringing the company into operation

- shaping the companies organization, structure and major processes
- shaping and setting up the administration business unit including the site & buildings division
- major contracts – site & buildings, business management contract with GSI GmbH, in kind contracts

General responsibilities

- full personal liability for the company's assets
- reporting to the shareholders assembly
- liaisons to shareholders, ministries and other stakeholders of FAIR
- liaisons to local authorities and the public bringing up a fully-fledged research facility – construction budget 1.6 billion€, expected yearly budget for operations 150 million€ joint management with the scientific managing director of the company yearly cash budget ramping up from 2 million€ (shortened financial year Oct.2010 – Dec. 2012) up to 44 million€ in 2012
- Personnel ramping up from 2 employees in Oct 2010 up to 35 in 2011
- set-up of the company
- Finances, accounting, purchasing, legal services
- all issues related to site & buildings, building permits, etc.
- general services
- personnel and recruitment
- technical safety and security

2001 – 2010 **GSI Helmholtzzentrum für Schwerionenforschung GmbH; www.gsi.de**

2009 – 2010 **Designated Administrative Director for FAIR, FAIR Division, Prokura (proxy holder on behalf of GSI GmbH)**

Within the GSI GmbH as designated major shareholder, host lab and providing the injector accelerators to the FAIR facility, the FAIR division has been established providing the seed for the company to be founded. I took over the responsibility to coordinate and account for all necessary work and preparations to start-up the company FAIR GmbH after the signature of the Convention for FAIR.

Key Achievements

- providing advice to the international community (in this respect the representatives to the prospective signatory countries – mostly research ministries or research organizations) to formulate the legal documents
- formulating the contractual framework for in-kind contributions
- preparing the SAP-ERP system of GSI to accommodate FAIR's accounting area independently
- pre-defining structures and processes for the FAIR GmbH

General Responsibilities

- proxy holder for GSI GmbH for all FAIR issues
- recruiting in advance for the FAIR GmbH

2006 – 2009 **Deputy Division leader FAIR Technical Division, Deputy Technical Project Leader Accelerator and Site & Buildings, Principal Investigator**

Focusing on the technical challenges of the FAIR project (accelerator construction and issues concerning site & buildings), I was Deputy for the assigned Technical Director for FAIR. The GSI's FAIR Division was holding five departments and almost 100 employees. The main focus of the Division laid on elaborating all specifications for the accelerator complex and the construction and development of site & buildings.

Key achievements

- implementing project structures for the accelerator sub-project
- recruiting key personnel for the newly formed site & buildings department
- implementing the central documentation and document management system for FAIR
- structuring of the project and the project documentation

General Responsibilities

- assuring the completeness and integrity of the specifications
- managing the accelerator subproject within the EU-FP7 preparatory
- phase program for FAIR I principal investigator within the Helmholtz
- Program "Structure of Matter" I managing the division on behalf of the division leader
- budgeting for the division

2001 – 2006 **Researcher Accelerator Division, Injectors Department**

GSI runs a large scale accelerator on a 7/24 basis for approx. 6000 hours/year. Within the linear accelerator and injector group I was the responsible liaison person to the controls department

Key achievements

- redesign and supervision of the implementation of the experimental beam line for the Super Heavy Elements (SHE) Program@GSI (discovery of new elements) and bringing it into successful operation
- requirements specification of the FAIR control system and machine protection systems

General responsibilities

- responsible machine physicist on duty for the linear accelerator
- accelerator coordinator on duty

- beam-line responsible for the SHE-beamline and general beam diagnostics
- requirements analysis and specifications for operating software and beam diagnostics elements Work package leader EU FP6 Program GANMVL
- supervisor for summer students

1996 – 2001 **Researcher, Institute for Nuclear Physics, Technical University Darmstadt**

I worked on my PhD thesis on the "*Design and Implementation of a Local Control System for the S-DALINAC*". This involved the designing of hardware boards, and involved me writing approximately 15.000 lines of code. The work comprised the completely new set-up of the local control system, but still to work together with the remote controls. I was also involved in the supervision of students at the University.

Key achievements

- implementing a new local controls system for the accelerator
- implementing a new rf-controls system (supervision of a diploma thesis)
- implementing a controls system for the Helium refrigerator (supervision of a diploma thesis)
- implementing an archiving database for accelerator settings

General responsibilities

- ensuring the operationally of the accelerator
- deputy IT-Manager of the institute
- supervision of diploma/master thesis
- co-supervision of PhD thesis
- supervision of the practical training of graduate students (lab work)